(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
4. November 2004 (04.11.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/095238 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2004/002194

(22) Internationales Anmeldedatum:
4. März 2004 (04.03.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 18 031.1 19. April 2003 (19.04.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DAIMLERCHRYSLER AG** [DE/DE]; Epplestrasse 225, 70567 Stuttgart (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KOBER, Heiko** [DE/DE]; Hauptstrasse 7, 75365 Calw (DE). **SCHNEIDER, Jutta** [DE/DE]; Kressbacher Strasse 12, 72072 Tübingen (DE). **SORG, Michael** [DE/DE]; Katharina-Schmitz-Strasse 20, 50226 Frechen (DE). **WIESER, Eva** [DE/DE]; Mörikestrasse 69, 70199 Stuttgart (DE).

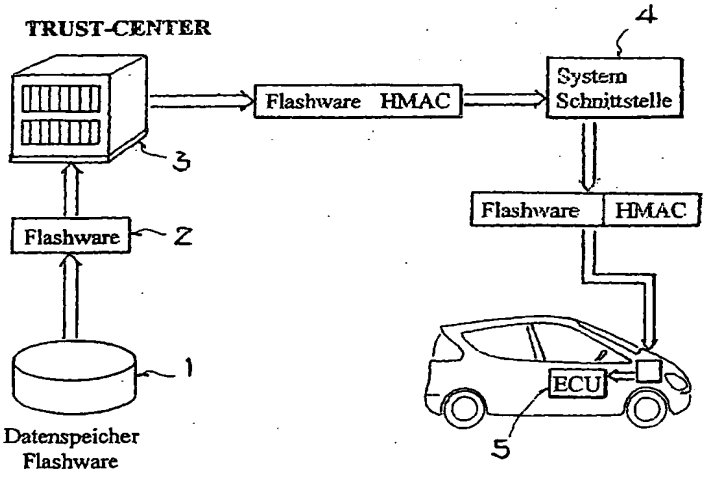
(74) Anwälte: **ESCHBACH, Arnold.** usw.; DaimlerChrysler AG, Intellectual Property Management, IPM-C106, 70546 Stuttgart (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GUARANTEEING THE INTEGRITY AND AUTHENTICITY OF FLASHWARE FOR CONTROL DEVICES

(54) Bezeichnung: VERFAHREN ZUR SICHERSTELLUNG DER INTEGRITÄT UND AUTHENTIZITÄT VON FLASHWARE FÜR STEUERGERÄTE



1... FLASHWARE DATA MEMORY
4... SYSTEM INTERFACE

(57) Abstract: The invention relates to a simplified symmetrical, cryptographic method which can be used as far as possible in all control devices of current motor vehicles. Said method is based on an authentication code which is calculated in a secured area, a trust center, by concatenating the application program, the flashware, with a secret data string and calculating a hash value from the concatenated application program, said hash value being calculated via both the application program and the secret data string. The hash value represents the authentication code for the application program that is to be tested. The authentication code is verified in the microprocessor system or the control device in which the application program is to be used.

[Fortsetzung auf der nächsten Seite]

WO 2004/095238 A1

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein vereinfachtes symmetrisches, kryptographisches Verfahren das auf möglichst allen Steuergeräten in heutigen Kraftfahrzeugen eingesetzt werden kann. Grundlage dieses Verfahrens ist ein Authentifizierungscode. Dieser Authentifizierungscode wird in einem gesicherten Bereich, einem sogenannten Trust-Center, berechnet, indem das Anwendungsprogramm, die sogenannte Flashware, mit einem geheimen Datenstring konkateniert wird und von dem konkatenierten Anwend ungsprogramm ein Hash-Wert berechnet wird. Dieser Hash-Wert wird hierbei sowohl über das Anwendungsprogramm als auch über den geheimen Datenstring berechnet. Dieser Hash-Wert ist der Authentifizierungscodes erfolgt in dem Mikroprozessorsystem oder in dem Steuergerät, in dem das Anwndungsprogramm eingesetzt weden so 11.